CLAIMS:

1. A method for protecting a digital good, the method comprising:

generating a fingerprint, the fingerprint being associated with a watermark;

embedding the watermark into a digital good without embedding the fingerprint.

2. A method as recited in claim 1, wherein the generating comprises producing a short fingerprint which is approximately equivalent to the fingerprint and is substantially smaller in scale than the fingerprint.

3. A method as recited in claim 1, wherein the generating comprises:

producing a pseudorandom watermark carrier that is independent of the watermark;

combining the carrier and the watermark to generate the fingerprint.

4. A method as recited in claim 1, wherein the generating comprises:

producing a pseudorandom watermark carrier that is independent of the watermark;

amalgamating the carrier and the watermark to generate the fingerprint.

5. A method as recited in claim 1, wherein the amalgamating comprises deriving the fingerprint from the carrier and the watermark.

6. A method as recited in claim 1, wherein the amalgamating comprises combining the carrier and the watermark to generate the fingerprint.

7. A method as recited in claim 1, wherein the fingerprint is uniquely associated with the watermark.

8. A method as recited in claim 1, wherein the fingerprint is at least partially derived from the watermark.

9. A method as recited in claim 1, wherein the fingerprint is associated with a detection entity.

10. A method as recited in claim 1, wherein the fingerprint is uniquely associated with a detection entity.

11. A method as recited in claim 1 further comprising:

segmenting the digital good into multiple segments;

repeating the obtaining, generating, and embedding for individual segments of the multiple segments, so that a segment has a segment-associated watermark embedded therein and a segment-associated fingerprint is associated with such segment-associated watermark.

12. A method as recited in claim 1, wherein the embedding produces a marked digital good, the method further comprising distributing identical copies of the marked digital good to multiple detection entities, wherein individual fingerprints are associated with one or more detection entities.

13. A method as recited in claim 1, wherein the digital good is selected from a group consisting of digitized images, digitized audio, digitized video, digitized multimedia, software applications, and media signals.

14. A modulated signal generated in accordance with the acts recited in claim 1, wherein the signal has a minimum collusion resistance that grows linearly with the scale of the signal.

15. A modified signal generated in accordance with the acts recited in claim 1, wherein the signal has a minimum collusion resistance that grows with the scale (N) of the signal in the order of magnitude of $O(N \log N)$.

16. A computer-readable medium having computer-executable instructions that, when executed by a computer, performs the method as recited in claim 1.

17. A computer comprising one or more computer-readable media having computer-executable instructions that, when executed by the computer, perform the method as recited in claim 1.

18. A method facilitating the protection digital goods, the method comprising:

obtaining a pseudorandom watermark;

producing a pseudorandom watermark carrier that is independent of the watermark;

amalgamating the carrier and the watermark to generate a fingerprint.

19. A method as recited in claim 18, wherein the amalgamating comprises deriving the fingerprint from the carrier and the watermark.

20. A method as recited in claim 18, wherein the amalgamating comprises combining the carrier and the watermark to generate the fingerprint.

21. A method as recited in claim 18 further comprising embedding the watermark into a digital good.

22. A method as recited in claim 18 further comprising embedding the watermark into a digital good without embedding the fingerprint.

23. A method as recited in claim 18, wherein the fingerprint is associated with a detection entity.

24. A method as recited in claim 18, wherein the fingerprint is uniquely associated with a detection entity.

25. A method as recited in claim 18, further comprising:

embedding the watermark into a digital good;

segmenting the digital good into multiple segments;

repeating the obtaining, producing, amalgamating, and embedding for individual segments of the multiple segments, so that a segment has a segment-associated watermark embedded therein and a segment-associated fingerprint is associated with such segment-associated watermark.

26. A method as recited in claim 18, further comprising generating a short fingerprint, which is approximately equivalent to the fingerprint and is substantially smaller in scale than the fingerprint.

27. A computer-readable medium having computer-executable instructions that, when executed by a computer, performs the method as recited in claim 18.

28. A computer comprising one or more computer-readable media having computer-executable instructions that, when executed by the computer, perform the method as recited in claim 18.

29. A method for facilitating the protection digital goods, the method comprising:

segmenting a digital good into multiple segments;

for one or more individual segments of the multiple segments:

obtaining a pseudorandom, segment-associated watermark;

generating a segment-associated fingerprint, the fingerprint being associated with the segment-associated watermark;

embedding the segment-associated watermark into its associated segment of the digital good.

30. A method as recited in claim 29 further comprising repeating the obtaining, generating, and embedding for the multiple segments of the digital good to produce a marked digital good.

31. A method as recited in claim 30 further comprising distributing identical copies of the marked digital good to multiple detection entities, wherein individual fingerprints are associated with one or more detection entities.

32. A modulated signal generated in accordance with the acts recited in claim 30, wherein the signal has a minimum collusion resistance that grows with the scale (N) of the signal in the order of magnitude of $O(N \log N)$.

33. A method as recited in claim 29, wherein during the embedding the watermark is embedded without embedding the fingerprint.

34. A computer-readable medium having computer-executable instructions that, when executed by a computer, performs the method as recited in claim 29.

35. A computer comprising one or more computer-readable media having computer-executable instructions that, when executed by the computer, perform the method as recited in claim 29.

36. A method facilitating the protection digital goods, the method comprising:

obtaining a fingerprint, wherein the fingerprint is not obtained from a digital good;

determining whether an embedded watermark is present in the digital good by correlating the digital good with the fingerprint.

37. A method as recited in claim 36, wherein the fingerprint is obtained from one of the group consisting of local memory, encrypted memory, firmware, and hardware.

38. A method as recited in claim 36, wherein the digital good is partitioned into multiple segments that may include a watermark and determining examines one or more segments of the multiple segments of the digital good.

39. A method as recited in claim 36, wherein the fingerprint is associated with a detection entity performing the determining.

40. A method as recited in claim 36, wherein the fingerprint is uniquely associated with a detection entity performing the determining.

41. A computer-readable medium having computer-executable instructions that, when executed by a computer, performs the method as recited in claim 36.

42. A computer comprising one or more computer-readable media having computer-executable instructions that, when executed by the computer, perform the method as recited in claim 36.

43. A method for facilitating the protection digital goods, the method comprising:

obtaining a suspect copy of a digital good;

obtaining a pristine, marked original copy of the digital good, this original marked copy having a watermarked embedded therein;

obtaining one or more watermark carriers, the carriers being collectively associated with the digital good but individual carriers being associated with an individual detection entity;

determining whether the suspect copy has been subjected to a collusion attack.

44. A method as recited in claim 43, responsive to the determining, further comprising indicating the suspect copy has been subjected to a collusion attack.

45. A method as recited in claim 43, responsive to the determining, further comprising identifying one or more members of a collusion clique.

46. A method as recited in claim 43 wherein the determining comprises correlating the suspect copy, the marked original copy, and one or more watermark carriers.

47. A computer-readable medium having computer-executable instructions that, when executed by a computer, performs the method as recited in claim 43.

48. A computer comprising one or more computer-readable media having computer-executable instructions that, when executed by the computer, perform the method as recited in claim 43.

49. A method for tracking digital goods, the method comprising:

attempting to access a watermark embedded in a digital good;

during such attempting, embedding one or more fingerprints into the digital good, wherein a fingerprint is associated with an entity.

50. A method as recited in claim 49, wherein the attempting comprises attempting to hide, alter, or remove the watermark from the digital signal.

51. A method as recited in claim 49, wherein the entity is a detection entity.

52. A method as recited in claim 49, wherein a fingerprint identifies an entity.

53. A method as recited in claim 49, wherein the entity is a detection entity.

54. A modulated signal generated in accordance with the acts recited in claim 49.

55. A computer-readable medium having computer-executable instructions that, when executed by a computer, performs the method as recited in claim 49.

56. A system for facilitating the protection of digital goods, the system comprising:

a key generation entity configured to generate pseudorandom watermarks and fingerprints;

a marker configured to embedded the watermark into a digital good, wherein the fingerprint is not embedded into the digital good.

57. A system as recited in claim 56, wherein the key generation entity is further configured to produce a pseudorandom watermark carrier that is independent of the watermark and combine the carrier and the watermark to generate the fingerprint.

58. A system as recited in claim 56, wherein the key generation entity is further configured to produce a pseudorandom watermark carrier that is independent of the watermark and coalesce the carrier and the watermark to generate the fingerprint.

59. A system as recited in claim 56, wherein the fingerprint is associated with the watermark.

60. A system as recited in claim 56, wherein the fingerprint is associated with a detection entity.

61. A system as recited in claim 56, wherein the digital good is selected from a group consisting of digitized images, digitized audio, digitized video, digitized multimedia, software applications, and media signals

62. A system for facilitating the protection of digital goods, the system comprising:

a digital-good obtainer configured to obtain a digital good;

a fingerprint memory configured to store a fingerprint;

a watermark detector configured to determining whether an embedded watermark is present in the digital good by correlating the digital good with the fingerprint.

63. A system as recited in claim 62, wherein the fingerprint is associated with the watermark.

64. A system as recited in claim 62, wherein the fingerprint is associated with the system.

65. A system as recited in claim 62, wherein the digital good is selected from a group consisting of digitized images, digitized audio, digitized video, digitized multimedia, software applications, and media signals

66. A system for facilitating the protection of digital goods, the system comprising:

a digital-good obtainer configured to obtain:

- a suspect copy of a digital good;
- a pristine, marked original copy of the digital good, this original marked copy having a watermarked embedded therein;
- one or more watermark carriers, the carriers being collectively associated with the digital good but individual carriers being associated with an individual detection entity;

a fingerprint detector configured to determine whether the suspect copy has been subjected to a collusion attack.

67. A system as recited in claim 66 further comprising a collusion indicator configured to indicate whether the suspect copy has been subjected to a collusion attack.

68. A system as recited in claim 66 further comprising a colluder identifier configured to identify one or more members of a collusion clique.

69. A system as recited in claim 66, wherein the fingerprint detector is further configured to correlate the suspect copy, the marked original copy, and one or more watermark carriers.

70. A computer-readable medium having computer-executable instructions that, when executed by a computer, performs the method comprising:

generating a fingerprint, the fingerprint being associated with a watermark;

embedding the watermark into a digital good without embedding the fingerprint.

71. A computer-readable medium having computer-executable instructions that, when executed by a computer, performs the method comprising:

obtaining a fingerprint, wherein the fingerprint is not obtained from a digital good;

determining whether an embedded watermark is present in the digital good by correlating the digital good with the fingerprint.

72. A computer-readable medium having computer-executable instructions that, when executed by a computer, performs the method comprising:

producing a pseudorandom watermark carrier that is independent of a pseudorandom watermark;

deriving a fingerprint from the carrier and the watermark.